Wallet-on-Wheels - Using Vehicle's Identity for Secure Mobile Money

Rebecca Copeland
Core Viewpoint, Kenilworth, United Kingdom

Noel Crespi (co-Author)
Telecom Sud-Paris, Evry, Paris, France

Abstract— Mobile Money is growing in the developed world while cars are becoming much smarter. Combine the two - and you get cars that 'own' a wallet. We propose not a user-centric, but a car-centric service that enables cars to have Pre-Pay subscription accounts for car-related purchases and for linking to financial services. The solution uses advanced car communications capability and securely stored car credentials to offer enhanced authentication security, which is a pre-requisite for such financial services. We propose strengthening the authentication procedure further with the 'Twin-Set' (of 'Two-Factor') method using both car-based and SIM-based authentication, and the 'Twin-Step' confirmation method for service authorization. In this paper we present an innovative use of advanced technologies, combining M2M, Mobile-Money, Automotive Communications and advanced security procedures.

Keywords- Mobile Money, M2M, UICC, TRE, MCIM, MCC901, SIM, NFC, IMSI, IMEI, OMA DM, PIN, cloning

I. INTRODUCTION

A. *Cars becoming 'phones'*

The automotive industry is undoubtedly mature, but one area is still evolving rapidly – vehicular communications. There has been much research devoted to exploiting M2M techniques when they are applied to the motor industry. There is particular good scope of growth in the area of user/driver applications, rather than vehicular M2M applications that rely on car sensors and internal systems). While smartphones become all-powerful, so do cars, once they are equipped with 3G/4G and WLAN communications. With advanced dashboard and NFC car-keys, user interfaces via touchscreens and buttons enable browsing, calling and streaming content. The question now is defining the boundaries and justifying any extra computing costs – not proving the technology. Taking advantage of both trends (smart cars and mobile money) we propose a more secure solution for drivers and car owners in WoW – Wallet on Wheels. The proposed solution utilizes car security and car connectivity to enable certain financial transactions and payments with added security.

B. *Mobile Money*

Mobile Money has been very successful in under-developed countries, providing banking facilities to remote regions and to populations that were previously underserved by the banks. The idea has also taken hold in the developed world, especially when cashless, contactless transactions are added to the package. The great inhibitors had been lack of collaboration with banks, lack of ecosystem of retailers, and lack of regulatory support. These inhibitors are now overcome in many territories. The Credit Card industry is evolving towards cardless phone-based payments. Financial services may be carrier-led [21,22] or bank-led [33]. Distinction should be made between applications: In developing countries, these services focus on mobile banking, but in the developing world the focus is cashless purchasing, replacing cash. Mobile Payments (mCommerce), Mobile Banking (e.g. money transfers) and eTicketing TravelCards.

C. *Why WoW?*

Car-related services are the primary range of applications that would benefit from cashless transactions – paying for petrol, tyres, garage services, road toll and parking. Many travel-related transactions, e.g. roadside kiosks payments and e-ticketing, are regarded as 'micropayments' that are too small for credit card. The next major application class is the car online facilities, including browsing and car entertainment. Dynamic services deliver navigation, road congestion and local information services that rely on geo-location positioning as well as mobile connectivity. General internet access is another car service, providing web based news and weather and any other internet sites for car users. Online car entertainment, like streaming music and videos, require ad-hoc payments or subscription fees. Lastly, remote banking transactions, i.e. 'Mobile Money', are most useful while travelling. This enables transferring money to car Pre-Pay accounts while checking on state of credit and viewing recent transactions. To support all that, several payment methods are needed, including on-demand payments and capped flat rate subscriptions.

Cars, unlike phones and laptops, are less prone to get lost, stolen or cloned. Car accounts, properly administered, are more long-lasting, as cars ownership is not as volatile as phone ownership. Greater trustiness is now in demand. There is increased threat to mobile computing, given the fast adoption of BYOD, as Symantec warns [1]. IBM [2] points out that Mobile-Money disruption is not about conversion of plastic transactions to the mobile devices, but the conversion of *cash* to cashless transactions. Mobile-Payment service facilitates micropayments, as App Stores do - once account details are in place, small payments become all too easy.

D. *Why now?*

In [8], a US Federal Reserve report states that "21% of mobile phone owners have used mobile banking in the past 12 months" and that "concerns about the security of the technology were the primary reason given for *not* using mobile payments (42%)". Previously, lack of ecosystems prevented the

adoption of early PoS (Point of Sales) cashless solutions. With the success of Mobile-Money applications in some regions, the service providers are solving the ecosystem issue by joining forces with credit cards companies [20], bringing credibility to the whole proposition. This opens up a huge network of retailers willing to accept cashless and cardless transactions.

The time is right for building on car communications. Cars are getting more intelligent, with on-board processing power and embedded capability of communications. The development of Automotive M2M applications has paved the way to low-cost car communication, and encouraged mobile networks to gear up for M2M signaling-heavy traffic. New cars are already equipped with embedded units that have connectivity facilities via the housed SIM (Subscriber Identity Module) cards, so that cars are becoming subscribers in their own right, through the partnering MNO (Mobile Network Operator).

Enhancing online services security is becoming urgent. There are worrying signs of growing credit fraud, especially cyber fraud, as warned by [25] and [26]. Latest security measures are not sufficient to stop the increase in such fraud. Hence, improved transaction security cannot come sooner. In addition, phone thefts are not abating either. In [27], cell phone theft in major US cities is declared as "a national criminal epidemic". It is likened to car stereo crime wave of the 1990s. The car stereo crime wave was eventually resolved by "the decision of car manufacturers to install higher-quality stereos at the factory". Similarly, the mobile industry should design measures that render stolen phones unsellable. Hence, safer financial applications by utilizing in-car secure authentication could help to combat these trends, for the automotive industry.

E. *Related work*

The opportunity for car applications is demonstrated by the long list of vehicular applications given in [7]. This study analyses connectivity protocols, but does not mention the need for security and does not include payment facilities. ETSI ITS (Intelligent Transport Systems) issued standards for vehicular communications applications [32]. BMW [3] has proposed car key fob contactless NFC-based services for small transactions, in particular for e-ticketing, in a similar way to the Oyster card in London, the Suica card in Tokyo and the Octopus card in Hong Kong. The key fob could also be used as a room key at a hotel, where the key code is downloaded to the fob [16]. In [4], architecture for several use cases utilizing NFC is proposed. It includes pairing of phones with the car's intelligence, as well as using the electronic car key outside the car, where NFC connectivity facilitates transferring personal purchasing authorization. Car connectivity includes more than just NFC protocols - Car WLAN and 3G/4G are also implemented in cars. In [5], GPS and GPRS are shown to be the fastest method for car-parking payments, compared with UMTS using mobile phones, due to greater delays when using the phone. In [6], IMS based Presence is proposed for discovery of cars WLAN, for a parking payment applications. IMS provides stronger security than in web services and more robust service control. In [9], automotive application platforms are evaluated for integration of smartphone. BMW's iDrive, Audi's MMI, Ford's SYNC and after-market Head Units such as Alpine are the fore-runners. Smartphone integration ensures that authentication underpins the linking of the phone, and that the car head unit can specify varying safety rules, e.g. in certain geographical locations and certain vehicle status. Thus, the car's head unit takes on the role of a 'security keeper'. Car intelligence has now moved on, to provide built-in communication intelligence hubs.

F. *This paper's contribution and structure*

We propose Wallet-on-Wheels as a vehicular version of Mobile-Money, Pre-Pay and Mobile-Banking applications. We show how greater security is provided via the vehicle-account authentication. This facility is particularly relevant for enterprises with a transport business or a car fleet to manage, and has a special application for the rental industry. In section II, the stake holders for car-related services are described, with their motivation to use WoW. In section III, the WoW account management is described, including the proposed car Pre-Pay facility. In section IV, the technology requirements and the proposed methods of enhanced authentication are discussed. In section V, the solution is summarized and issues are discussed. In VI - the final word.

II. THE CONCEPT OF WALLET ON WHEELS

A. *Stakeholders*

In setting up an automotive Mobile-Money service, several stake holders must come together, and they all must be equally motivated to deliver a successful service. The leading application SP (Service Provider) may be the Automotive Manufacturer, their agents - Automotive SP, the mobile-Money SP or the MNO. Some Pre-Pay services can be managed in house by MNOs or SPs, but full banking and credit facilities require the involvement of Mobile-Money specialist. In all cases, mobile communications is requires, so network providers must be involved.

The *Automotive M2M Equipment Supplier* (AMES) owns the car embedded module that contains communication software, and they - or Automotive SPs, operate a range of car-specific applications. *Figure 1* shows Automotive-centric service, where the automotive party has the relationship with the financial service providers. The mobile operator facilitates the communication for the transactions and for the delivery of online devices.

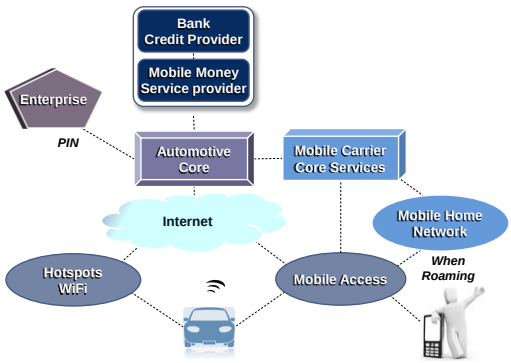

Fig. 1. Automotive manufacturer operating WoW

Automotive manufacturers provide a growing range of car-related services, and have strong motivation to enable WoW for their cars. Their main aim is to add features to their cars via attractive services and facilities. While they get paid for such services, the main benefit is still selling cars. Without adequate means of flexible charging, they are constraint by what they can offer. Furthermore, web-based car entertainment (streaming or downloading music and videos) changes the perspective of car-user spending and more innovative services can now demand higher fees. New services can add value even to second-hand cars, so promotional credit towards these services is a useful option to any car seller. Such vouchers can be distributed by an ecosystem of retailers and agents.

Mobile Network Operator (MNO) provides network services to the car and to the user's phone whilst in the car. MNOs may have competing services to those offered by AMES and could provide WoW to cars in the same manner as to phones. MNOs' first concern is growing their phone subscription base. The cars are themselves mobile subscribers, with their own SIMs, and they represent an additional customer base. Providing improved security platform for a multitude of financial services can be a real differentiator against current web service providers that dominate the market today. For MNOs, car accounts that are independent of the car owner are more stable since they do not churn as much as smartphone accounts. Especially attractive are large enterprise accounts, where employees' spending is controlled by their organizations. *Figure 2* shows a WoW solution that is operated by an MNO. The MNO could provide some independent car services without the automotive manufacturer, but this may jeopardize their business with partnering automotive service providers for other types of car communications.

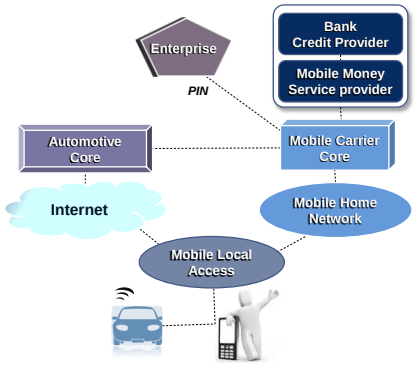

Fig. 2. MNO operating WoW

The *Mobile-Money Service Providers* (MMSPs) are software specialists that developed cashless transaction systems. These systems may have evolved from the early Intelligent Network Pre-Pay systems and the later OCS (Online Charging System). Their links to credit replenishment agencies have evolved into partnerships with credit card and banking companies that underpin the financial arrangements and encourage retailers to participate. The MMSPs business model relies on high volume of business, where they are paid a small fee per transaction. That fee is shared with the banks or credit agencies. While taking a margin of 30% per transaction seems high, it is not seen as such by ad-hoc payees seeking convenience, especially when it is applied to small amounts.

The *Car Account Holder* (CAH) is the car owner that subscribes to WoW with either MNO or AMES. The accounts are associated with the car, and could be set up when the car is bought, or when the service is initialized. The subscription is either associated with a credit card or bank details. Alternatively, account holders can authorize a credit amount and replenish it when it is exhausted. Anonymous online CAH Pre-Pay service can be operated by selling redeemable vouchers which are associated with the car registration. CAHs can be enterprises with a car fleet or car-pool, where the organization has a single subscription that is shared via multiple user accounts. The enterprise motivation for subscribing to WoW is reducing travel expenses as well as administration costs: enterprises benefit by managing budgets and negotiating bulk discounts for car fleet services and reduce administration costs, since there is no need for employees to submit claims. As this is cardless as well as cashless, card administration is redundant.

III. THE WOW ACCOUNT MANAGEMENT FACILITIES

A. Car Payment Methods

WoW is intended to be a platform for multiple types of accounts and a variety of charging methods. A diverse range of services needs a wide range of charging methods. *Table 1* describes the type of services and the payment modes. With this range of charging methods, WoW does not have to be restricted only to car-related services. However, unlike phone Mobile-Money, the pre-requisite for WOW is car ownership.

Table 1: Automotive Charging Methods

	Method	*Scope*	*User/Usage*
1	Free Services	Emergency 'eCall' (free if it is regulatory)	Mandatory
2	Packaged Lifetime Services	Breakdown services Call Centre, Driver Assistance	Low usage
3	On-demand Service	Per download charge, e.g. Navigation maps.	Car-specific
4	Capped flat rate, Subscription	Traffic information Location-based services	Per car owner
5	Pre-Pay Car Credit	Any chargeable service	Any car user
6	Post-Pay Car Account	Any charged service	Enterprise or Family
7	Post-Pay User Account	Personalized range of services	Per person

B. Car Subscriptions Options

Subscription is the mechanism that enables authentication and spending authorization. An 'Account' is defined as managed credit and payments facility. A car user may be a temporary or permanent driver, who is entrusted with a certain spending power up to a given level. There can be several types of relationships between accounts, subscriptions and users, as shown in *Figure 3*. In option A, users share a single account and subscription e.g. family members. In option B, multiple users have individual accounts but a single subscription e.g. car hire or enterprise funded accounts. In option C, separate

subscriptions and separate accounts apply to shared cars, e.g. anonymous vouchers or short-term car rental.

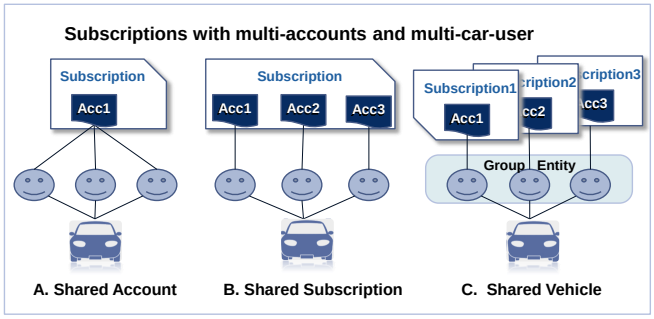

Fig. 3. Relationships of subscriptions

C. Car Pre-Pay Service

Phone users have either a named contract account or contract-less Pre-Pay accounts. The same choices should also be available to car accounts. A Pre-Pay service for car accounts (not personal accounts) could be an attractive service to car owners. The service allows anyone to add credit using personal credit cards. Casual or temporary drivers have access to all services that are paid for, simplifying the process of changing drivers. Remaining credit could stay with the car for the next driver, or withdrawn using the same portal with the same credit card credentials. This type of accounts makes it possible to add more services (in-car entertainment: streaming audio books, music and video etc.) at any time, so it increases the opportunities for obtaining subscriptions. Just as Pre-Pay phones broke the barrier of signing contracts, so could a WoW Pre-Pay cars break the barrier of taking on new car services.

Unlike the practice today, the credit can be used for any chargeable service, with no need to specify upfront what services are purchased. This empowers car users to prioritize consumption according to their preferences, and gain more control over charges. The versatility of WoW overcomes user resistance to having more special accounts for special services that are used only occasionally. It is also useful for car owners controlling spending by other drivers, e.g. family members, office pool cars or rental cars.

A car Pre-Pay account can be set to allow anyone to add credit and anyone to spend it, which is useful for promotions and for service introductions. Credit vouchers that can be purchased by anyone on behalf of any car can be given as gifts. Vouchers can also be used for promotions of new services, i.e. providing a limited credit as service introductory packages. Such vouchers can be issued at the time of a service launching, or provided when a new car user is established. Car rentals firms can package them together with their rental deals. Enterprise pooled cars may be allowed certain amount of credit that the enterprise would fund for the employees, but the employees could easily add more voucher credit, if so wished.

It is possible to run such a service alongside flat-rate or fee-free services on the same SIM card, operating a Pre-Pay application with a structured user profile. A WoW Pre-Pay communication usage service (e.g. streaming contents) needs to authenticate the user credentials and retrieve user's service profile. It has to monitor session start/close events, so as to charge for usage and apply the appropriate charging rate when calculating the spent amount. For WoW transactions, the service verifies the amount and the recipient at the PoS, gets user confirmation and sends back a notification of a completed transaction. The credit levels are adjusted and the user is notified when the credit is used up, giving an option to replenish it. This functionality is the same as traditional mobile Pre-Pay service, but it is car-centric, not person-centric.

D. Use Case Call Flow

Dynamic cross-entity communications in the course of service delivery is no longer an issue but should be minimized, for both performance and security reasons. A WoW service does require cross-party links, as in the case of WoW service via an AMES. The MNOs are chosen in the territory where the car is going to be sold, and their SIM identity and credential materials are embedded in the special sealed unit. When the car is sold, the AMES also sells a package of car services, including WoW. In the case of an enterprise customer, the car is allocated to employees temporarily or permanently, and the user is given a PIN. The call flow for authorizing a transaction requires collaboration, as is shown in Figure 4.

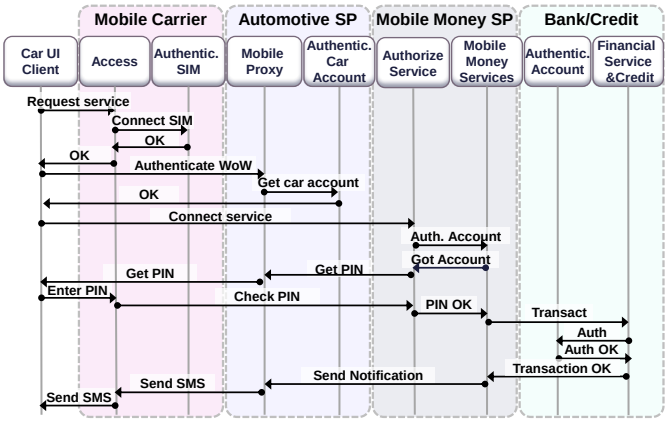

Fig. 4. Call flow for automotive-centric use case

The authentication of the SIM by the MNO is used for charging for the communication part of the service. The account number and PIN are used to authorize the transaction. Linking both processes can provide a much stronger authentication procedure, since the car credentials are very well protected. There is no need for dynamic access to the enterprise server if a synchronized list of PINs is kept by the service provider. The provisioning of PINs in a separate link, which is used only occasionally, is much safer.

E. Car Account Issues

There are several issues in managing changes of car owners and users. There must be a procedure for severing the previous association (e.g. between personal phone number and car SIM). If car ownership is tracked, a change of ownership will trigger this procedure, even if a new association is not created. The handling of remaining credit can then have several options: credit amount transferred to another car account; credit is left with the car for the next owner; reclaim credit via the same

credit card; or old credit amounts purged by the service provider, depending on local regulations.

Various consumer laws dictate that payment authorization must be associated with a named person, in order to ensure 'culpability', relating spending to a responsible person. Therefore, shared car usage and their transactions must be tracked, audited and confirmed to avoid 'deniability'.

Associating cars with owners' identities enhances trustiness. The registration of cars ownership is mandated by law and is well maintained in most countries, but the information is not universally opened to service providers. Users are requested to enter car registration when subscribing to services, but this does not tie the user details to the car. The payers' details are known to the banks, but not necessarily to the service provider, thus linking payer's name and address to car owners cannot be taken for granted.

IV. Car Technology Facilities

Car communication technology is evolving fast. Car dashboards are becoming more powerful and more flexible, with touch screens and programmable buttons. The user interface must be able to engage the user in a short dialogue that selects and executes a transaction. As an alternative UI (User Interface), phones that can be tethered to the car local network could be used as terminals for WoW application.

A. Car Connectivity

The WoW services must be ubiquitous, operating wherever the existing car communications can access the Internet. Many exiting quality cars already have full mobile connectivity, including 3G/4G and legacy communication, offering Internet services, especially for breakdown and emergencies. Car connectivity is paramount when the standard EU 'eCall' becomes mandatory in 2015, by new EU regulation [29]. This means that cars must have legacy Voice capabilities, until the countries' emergency agencies can reliably receive VoIP calls.

As most financial services are using messaging for personal authorization, a car messaging service must be available. Such messages can be traditional SMS (Short Messaging Service) or IP based messaging. SMS is needed for transaction confirmation and non-repudiation. Such messaging facilities also provide an audit trail.

The car WLAN provides inter-device communication and the tethering of phones to the car modules. The car WLAN range enables transactions to be made in the vicinity of the car, such as petrol station shops and roadside kiosks, using local connectivity only. Cars may connect to nearby hotspots, enabling Internet access without using the carrier's mobile network at all, yet providing full connectivity for WoW transactions. This is particularly useful for enterprises, where cars can be attached to their corporate network, opening up a number of new possibilities, such as downloading content to cars for perusal later on, checking on parked cars status (e.g. lights left on), checking car parking spaces and more. However, such hotspots connectivity is not ubiquitous and requires a separate agreement to pay communication costs.

B. Car Trusted Environment (TRE) – embedded UICC

The standards [15] have defined generic requirements for M2M Trusted Environment (TRE), which is tamper-proof. The car sealed communication unit is a module that is fixed into the car frame during car manufacturing. It contains embedded UICC (UMTS Integrated Circuit Card) with a SIM card from an MNO. This unit is then sealed and cannot be tampered with once the vehicle has left the factory. This fully secure embedded UICC is the key to the idea of WoW that enables superior security for authorization of transactions. It may be possible to build a dashboard card reader to recognize any MNO's SIM, but this does not benefit from the built-in secure car communication SIM.

C. Car Global Identity

For the car to have a globally unique and routable identity in mobile networks, it needs an MSISDN (Mobile Subscriber Integrated Service Data Network) identity of a mobile user, which is provided by a partnering MNO when they allocate a SIM to be inserted in the car embedded module. This identity is linked to a particular country, but when cars are shipped to other territories, they 'roam' for their entire life, increasing communication costs considerably. Since changing the SIM card in the sealed unit will compromise the security of the embedded UICC, a mechanism is needed to allow multiple MNO networks to serve one SIM. For this reason, automotive manufacturers seek independent allocation of global addresses, which are not country-specific and do not need to change when crossing borders. MNOs with a growing population of M2M devices, which have the same problem, are also looking for global identities. This facility is enabled by the ITU Recommendation E.212. Global SIMs were conceived originally to support maritime, aerospace and geographically dispersed activities, but the advent of M2M devices has brought fresh interest. The ITU can now grant global MCCs (Mobile Country Codes), known as MCC 901, that is not associated with any country. It enables global routing of traffic to the designated home network, regardless of locations, and in effect treating the operator as native in every country. To date, only few operators have been granted global MCC numbers. Among them, Orange [21] and Vodafone [22] who are now offering global SIMs to international M2M businesses.

D. Secure Authentication Procedures

Embedded SIM: The SIM is placed in the sealed UICC unit with authentication materials, i.e. the 'K' parameter (shared secret) and processing algorithms. As for mobile phones, the MNO authenticates the car by the IMSI (International Mobile Subscriber Identity), treating the car as a mobile subscriber. This enables the car to communicate over mobile networks, both legacy and broadband. The car IMSI is only known to MNOs, and they can use it to authorize services. Alternatively, additional serial numbers and security credentials can be stored in the embedded unit and used solely for WoW car authentication. While phone contracts associate SIM identity with named accounts, the car SIM is currently assigned to the car without tracking of owners. The car Pre-Pay account can be used in such cases, with anonymous accounts, where names and banking details are known to the service providers (AMES

or MMSP) but not the carrier, if the car communication is charged separately.

Firmware Security: The Car IMEI (International Mobile Equipment Identity) is a serial number that is stored in the sealed unit, together with the shared secret and is used to create security keys for car-specific authentication. Embedding these credentials in the firmware, which is welded to the car frame and sealed over, makes it impossible to clone. This is intended to prevent the 'IMEI syndrome' from happening again. IMEI was formerly used as a firmware serial number that uniquely identified the handset equipment and linked the (IMSI) with the terminal. However, due to widespread cloning of device boards with their IMEIs, as reported in [12], the IMEI is no longer guaranteed to be unique and cannot be used for authentication. This is not the case for cars with TREs. The car serial numbers and credentials are securely stored in this tamper-proof unit, and are safe to utilize. Several alternative sets of credentials should be stored in this protected module, for future use, if and when required.

Twin-Set Authentication: The idea of the Twin-Set (also called Two-Factor) Authentication, is to link two independent sets of credentials in the authentication. This is often achieved via a fob with disconnected generation of security codes. Identity based fraud is frustrated by this mechanism if the fraudsters cannot get hold of both items. Thus, using separate car serial number (IMEI equivalent) and separately stored credentials can be used with the car's SIM authentication to authorize WoW transactions. To separate the MNO area from car applications, a second TRE can be integrated into the car frame separately, making cloning even harder.

Twin-Step Authentication: This principle requires a confirmation response on an alternative device or interface, e.g. changing passwords for web applications requiring confirmations via email or mobile text. This makes it harder to copy or guess, since the fraudster needs access to both accounts. Thus, car authentication can be strengthened by mobile phones confirmations. The phones need not be tethered to the car, but the association with the mobile phone number has to be safely recorded, in a secure procedure.

PIN authorization: A PIN can be assigned by the application to individual users or managed by the enterprise or the car rental company. It is possible to operate a simple car-account with no PIN, for greater ease-of-use. Such Pre-Pay accounts can be used by pool cars and short rental, for low value transactions. Obviously, it is less secure. Stolen cars with no-PIN-accounts will allow thieves to use existing credit until such time that the WoW service is notified or the credit is exhausted. This can be avoided by temporary PINs, where expiry is triggered by elapsed time or by depleted credit. PINs are also necessary in some countries to comply with parental control regulations. Using multiple PINs per account, the account holder can vary the levels of access for other car users.

E. Secure Provisioning of Credentials

To enable cars to be securely authenticated by a WoW service, the credentials should be set up in a separate procedure, avoiding transmitting them 'over-the-air', which can be intercepted or subverted. The credential must be shared by both parties, to generate the necessary security keys and certificates in parallel. The initial setup stage is the most vulnerable phase of the process and must be undertaken only in the rare occasions of instituting a new relationship, i.e. when the service is initialized or when a new owner chooses a different service provider. The procedure of exchanging credentials for M2M devices was the focus of the 3GPP Technical Report (TR) 33.813 [15]. This TR was motivated by requirements to change MNOs for M2M devices, since the MNO's SIMs are fixed during manufacturing and not at service initialization time. This TR, which has been last updated in 2010, is not going forward because of worries that revealing subscriber authentication keys to any 3rd party will result in various types of fraud. The concerns are greater because not only internal numbers (IMSI) are vulnerable, but also procedures and algorithms used widely elsewhere. Due to the gateway capability in such devices, the impact of compromised security is even greater. If backward compatibility is to be supported over the car lifetime, the MNOs' ability to introduce new security algorithm is considerably reduced. For all these reasons, MNOs argue that the simplest method, which is also the most cost effective, is what is already available - a removable SIM. However, this method, which satisfies the needs of portable M2M devices, is by no means secure enough for vehicles with a great range of services and greater scope of spending. The automotive industry requires changing SIM identity and credentials in the embedded UICC without physically gaining access to the SIM firmware.

In the TR 33.813, MCIM (M2M Communication Identity Module) is defined, with security features that are based on USIM (UMTS SIM) and ISIM (IMS SIM). To enhance security of the air communication procedures for MCIM setup, it is recommended to use secure channels as specified in ETSI TS 102 484 and 3GPP TS 33.110. To support a long car lifetime, the number of potential credentials should be unlimited. Ideally, the entire procedure should be remotely executed by a trusted agency, an independent PVA (*Platform Validation Authority*), which will manage the inter-party exchanges. This method requires a service discovery procedure and new registration functions that are yet to be accepted as standards and are not universally implemented. All MNOs must support OMA (Open Mobile Alliance) DM (Data Management) procedures and PKI (*Public Key Infrastructure*). Although it is reliable and flexible, this method is not likely to be available for a long time yet.

A more practical solution is based on pre-storing all the credentials and procedures in the embedded unit, with no need for a central authority, minimizing the transmission of sensitive information. The new IMSIs, new car serial numbers, associated algorithms and pre-configured shared Secrets should be all pre-stored on the sealed UICC before the car leaves the factory. Each time a change of MNO or a WoW account is performed, another set of keys and codes are used from the given lists. This solution needs more memory for storing the multiple algorithms, but there is a significant advantage in avoiding the transmission of credentials over the air.

The issue of changing MNO and changing WoW accounts are similar but should be viewed as separate procedures, occurring at different times. The credential initialization

mechanisms can use the same method, but it is advisable to have a separate store of embedded credentials for WoW. Mobile IMSI is not divulged to phone users, and the car IMSI (in the MNO's SIM) is not divulged to car owners or account holders. If the car IMSI is not available for the WoW service provider, the additional embedded serial numbers and credentials will be used for a separate WoW authentication.

F. NFC Based Car Key fob Applications

Electronic car key fobs allow opening car doors and starting the engine without inserting a key in a keyhole, using Near Field Communications (NFC). Such keys could be used for more functions, as described in [3]. However, the key fobs have all the issues of smartphones (get lost or stolen, need battery) but few of the advantages, particularly regarding the UI. Electronic car key cloning has become a serious problem recently, as reported in [32]. Financial services and commercial transactions need far greater security and reliability. NFC key fob applications could still benefit from WoW, by enabling more secure in-car replenishment of credit in the fob, using WoW authentication. This allows for small credit amounts to be downloaded to the fob, perhaps for a set period of time, thus using the fob as a user interface for WoW.

V. SOLUTION SUMMARY

A. The proposed Accounts

The scope of WoW applications will be determined by service providers wishing to benefit from this car-secured platform. WoW is well suited for hire cars, car pool and car fleets, i.e. cars belonging to a company that are driven by temporary drivers. We have highlighted several examples, including funded accounts for corporate transport business, individual capped accounts for car-dedicated services, ad-hoc limited credit subscriptions to introduce new services, and more. The type of accounts ranges from anonymous Pre-Pay vouchers to fully tracked ownership.

B. The Proposed Authentication Scheme

Procedures for initiating and activating subscriptions of WoW service require stringent procedures, considering the rising identity thefts (SIM), cybercrime (air interface) and cloning (firmware). We propose to extend the existing sealed unit with a separate set of credentials that are dedicated to the car authentication. While SIM provision is controlled by the MNO, the car serial numbers are managed by the Automotive Party. The use of TRE firmware, which is already in production by car manufacturers, is adding a level of security that is not available in portable devices, such as phones, laptops and tablets. Secret serial numbers (equivalent to IMEI) can be used as a separate non-SIM authentication method and the combination of this with the embedded SIM authentication will strengthen the procedure considerably. We propose to use an MCIM technique for provisioning of credentials, where identification numbers and shared secrets are pre-stored on the TRE tamper-proof module. These serial numbers can be changed, if necessary, using MCIM standards.

The car communication services are authenticated by the MNO core systems, using the MNO's owned SIM. The WoW service is authorized via the car's serial number in an independent authentication. The two procedures can co-exist, but it is also possible to fuse them, using both the car serial number and the MNO's IMSI number in the security hashing procedure that produces authentication keys for both WoW and MNO communications. This will achieved the *Twin-Set* authentication principle that links separate, independent credentials, to prevent copying. The method of *Twin-Step* confirmation can also be implemented, through confirmation responses via alternative accounts, e.g. the user's mobile phone or email account. Although any mobile phone can be tethered, only the pre-stored phone number belonging to the account holder will be used as confirmation. In addition, the car key fob can still be used safely with downloaded small credit amount, like contactless e-ticketing, where WoW is used to transfer credit to the key fob. *Figure 5* demonstrates the relationships between the Phone SIM, car serial number and key fob.

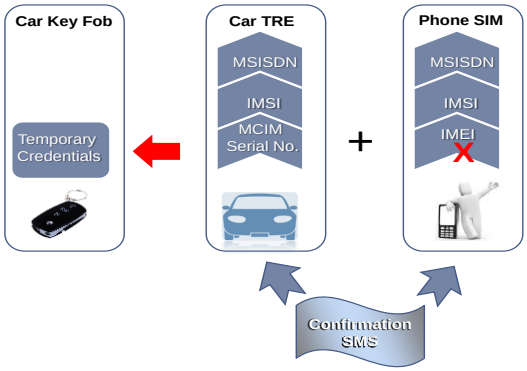

Fig. 5. Secure Authentication by using MCIM serial numbers and IMSI

C. Solution Issues and Weaknesses

Smartphone mobile money has several advantages over WoW. Compared with smartphones, WoW users are restricted to authorized car drivers and car enabled applications, while smartphone Mobile Money users have personally customized services that have no connection with car ownership. However, using the car identity, greater security is offered that is lacking on smartphones. We see WoW as a set of services that is focused on automotive applications, satisfying travelling needs.

One of the difficulties faced by automotive manufacturers is bringing innovation to the existing car population. Cars have long lifecycle - much longer than hi-tech devices. The spread of new applications with new technology, such as WoW, is constraint by the rate of selling new cars. Future requirements should be anticipated by manufacturers, and the ability of downloading upgrades should be supported. However, such flexibility increases risks of tampering and corrupting the car safe area.

The WoW service brings together several types of technologies and several partnering stakeholders, as shown in Figure 6. This may increase the complexity of delivering a unified service, because it relies on collaboration. However, the different technologies (financial transaction processing and pre-pay/credit, car embedded communications, security

procedures, network connectivity) are handled by their respective stakeholders, with a common aim to enhance services. The issue of suitable business models is also being resolved, whether the service is led by an automotive manufacturer, automotive SP, MNO or independent Mobile Money service providers, by acknowledging the contribution of all the parties and setting up mutual remunerations.

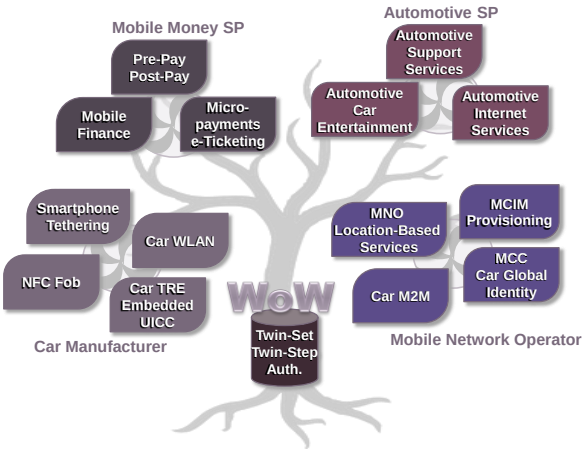

Fig. 6. WoW mix of technologies and participating stakeholders

VI. FINAL WORD

Wallet-on-Wheels is a practical solution to travelling related financial services, including money transfer, micropayments, in-car entertainment, driver support services and more. The idea of WoW is not merely to provide improved car-related paid services or budget-controlled shared car accounts, but also to offer higher security platform, especially in the light of increasing fraud and identity thefts. Hence, this paper proposes two novel ideas that are interwoven in the proposed WoW solution: a) cars can 'own' accounts (Pre-Pay or Post-Pay) and b) car based authentication increases security for financial services. The success of this idea depends not on one technology, but the collaboration of the stakeholders, bringing together a number of mechanisms.

REFERENCES

[1] N Severino"A New Approach to Mobile Security: Protection on Every Side", Symantec, Connect World LA 2011

[2] A Jimenez "Mobile Money Roadmap for Latin America" IBM, Connect-World LA 2011

[3] BMW, T Kratz 2011 "The BMW NFC Key" http://www.pocket-lint.com/news/38232/bmw-nfc-key-fob-wallet; http://www.elektroniknet.de/automotive/komfortelektronik/artikel/26368/1/;http://www.thesundaytimes.co.uk/sto/ingear/cars/Driving/article543577.ece ;

[4] R Steffen, J Preißinger, T Schöllermann, A Müller, I Schnabel "Near Field Communication in an Automotive Environment" IEEE 2010

[5] G Benelli, A Pozzebon, R Sesto "Different wireless technologies for the remotepayment of street car parks" IEEE 2012

[6] A De Rogatis, R Garufi, A Robustelli, P Addesso, M Longo "An Automatic-Payment Parking Service Integrated within the 3G-IMS Architecture" IEEE 2009

[7] K Dar, M Bakhouya, J Gaber, M Wack "Wireless Communication Technologies for ITS Applications" IEEE 2010

[8] US Federal reserve "Consumers and Mobile Financial Services March "

[9] Nokia Research Centre "Morphing Smartphones into Automotive Application Platforms" IEEE 2012

[10] H Bender, G Lehmann "Evolution of SIM Provisioning Towards a Flexible MCIM Provisioning in M2M Vertical Industries" IEEE, 2012

[11] OECD (2012), "Machine-to-Machine Communications: Connecting Billions of Devices", OECD Digital Economy Papers, No. 192, OECD

[12] L Barria, B Smeets, K Sallberg "M2M Remote-Subscription Management" The Ericsson Review (January 2011)

[13] W Cao, C Lin, W Zhou, F Sun "A Real-Time Planning-based Scheduling Policy with CAN for Automotive Communication Systems" IEEE2008

[14] W Vandenberghe, I Moerman, P Demeester "On the Feasibility of Utilizing Smartphones for Vehicular Ad Hoc Networking" IEEE2011

[15] 3GPP TR 33.812 "Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment" (Release 9) 2010-06

[16] NFCworld S Clarck "BMW uses NFC car keys to open hotel room doors" http://www.nfcworld.com/2012/04/23/315235/bmw-uses-nfc-car-keys-to-open-hotel-room-doors/

[17] C Tchepnda, H Moustafa, H Labiod, G Bourdon "Prioritizing and Enhancing Vehicular Networks Authentication Process Using DSRC Channels Diversity" IEEE2008

[18] X Lin, X Li "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks" IEEE 2013

[19] J Teo, L Ngoh, H Guo "An Anonymous DoS-Resistant Password-based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks" IEEE2009

[20] VisaEurope "Visa Europe backs Mobile Money Network" http://www.visaeurope.com/en/newsroom/news/articles/2012/visa_europe_backs_mmn.aspx

[21] Informa October 2011 http://www.telecoms.com/34650/france-telecom-to-launch-m2m-sim-on-shared-mobile-country-code/

[22] Vodafone m2m.vodafone.com/discover-m2m/why-vodafone-m2m/

[23] Vodafone to offer M-Peza in India http://www.mobilemarketingwatch.com/vodafone-bringing-Mobile-Money-services-to-india-31676/

[24] UK Card Association, March 2013 "decline in fraud losses stalled by rise in deception crimes aimed at consumers"

[25] Yahoo Finance March 2013 http://finance.yahoo.com/news/top-states-credit-card-fraud-090048490.html

[26] The Time Magazine 2013 "Law Enforcement Sounds Alarm on Cell-Phone-Theft Epidemic" http://swampland.time.com/2013/03/25/law-enforcement-sounds-alarm-on-cell-phone-theft-epidemic/

[27] Cloning car keys http://www.autoexpress.co.uk/bmw/60264/bmw-owners-offered-fix-hi-tech-theft

[28] "BMW owners offered fix for hi-tech theft" september 2012 autoexpress.co.uk/bmw/60264/bmw-owners-offered-fix-hi-tech-theft

[29] "EU adopts automobile emergency calling service eCall" ,2011 http://www.telecompaper.com/news/eu-adopts-automobile-emergency-calling-service-ecall--825732

[30] BBC news 2011 "Electronic car key fobs fail" http://www.bbc.co.uk/news/uk-england-hampshire-15278838

[31] 3GPP TS 33.402 "3GPP System Architecture Evolution (SAE), Security aspects of non-3GPP accesses (Release 11)" (2012-06)

[32] ETSI TS 102 637-1 V1.1.1 "Intelligent Transport Systems (ITS) - Vehicular Communications Basic Set of Applications Part 1: Functional Requirements" 2010

[33] Barclaise Mobile Banking http://www.barclays.co.uk/MobileBankingServices/MobileBanking/P1242561069586